<u>**REMARKS / ARGUMENTS**</u>

Claims 1-24 are pending in the instant application. Claims 1 and 12 are independent. Claims 2-11 and 13-24 depend from independent claims 1 and 12, respectively.

Claims 1-24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over USP 4,896,934 ("Arthurs"), in view of USP 7,151,777 ("Sawey"), and further view of admitted prior art of USP 6,658,002 ("Ross"). The Applicant respectfully traverses these rejections at least for the reasons previously set forth during prosecution and at least based on the following remarks.

REJECTION UNDER 35 U.S.C. § 103

The MPEP states the following regarding the requirements for establishing a *prima facie* case of obviousness:

> The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

See the MPEP at § 2142, citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006), and

KSR International Co. v. Teleflex Inc., 82 USPQ2d at 1396 (quoting Federal Circuit

statement with approval). "The mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art" *See id.,* § 2143.01. Furthermore, in order to render the claims obvious, the asserted prior art combination must **teach or suggest each and <u>every</u> claim feature**. *See In re Royka*, 490 F.2d 981 (CCPA 1974) (to establish *prima facie* obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art)[1]; *see also In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (A proper obviousness determination requires that an Examiner make "a searching comparison of the claimed invention – **including all its limitations** – with the teaching of the prior art.")

If a *prima facie* case of obviousness is not established, the Applicant has no obligation to submit evidence of nonobviousness:

> The examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness. If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness.

See MPEP at § 2142.

With these principles in mind, the Applicants now turn to the claim rejections in particular.

---

[1] Emphasis added except where noted otherwise.

I.   **The Proposed Combination of Arthurs, Sawey and Ross Does Not Render Claims 1-24 Unpatentable**

A.   **Independent Claims 1 and 12**

With regard to the rejection of independent claim 1 under 35 U.S.C. § 103(a), the Applicant submits that the combination of Arthurs, Sawey and Ross does not disclose or suggest at least the limitation of "generating a physical port security bit map of allowed destination ports, wherein said physical port security bit map is generated based on one or both of information in said received frame of digital data and/or port security information associated with said network device; comparing, using at least one logical operation, said destination port bit map with said physical port security bit map to generate a bit map of allowed destination ports," as recited by the Applicant in independent claim 1.

A(1) Arthurs Does Not Disclose "Generating a Destination Port Bit map", "Generating a Physical Port Security Map" or "Comparing …Said Destination Port Bit Map with Said Physical Port Security Map to Generate a Bit Map of Allowed Destination Ports"

The Office Action (see page 3) states the following:

Referring to claim 1:

i. Arthurs teaches: A method of providing physical port security in a digital communication system, comprising:

receiving a frame of digital data at a network device (see figure 3 'packet format', of Arthurs);

a destination port bit map based on the destination address information contained in said frame of digital data (see figure 3, element 'destination bitmap field'; and column 5, lines 50-54, of Arthurs);

generating a physical port availability bit map of allowed destination ports, wherein said physical port availability bit map is generated based on one or both of information in said received frame of digital data and/or port security information associated with said network device (see column 5, lines 58-65; column 6, lines 4-9; and column 7, lines 1-3, of Arthurs);

comparing, using at least one logical operation, said destination port bit map with said physical port availability bit map to generate a bit map of allowed destination ports (see column 5, lines 58-65; column 6, lines 4-9; and column 7, lines 1-3, of Arthurs); and

forwarding said frame of digital data to one or more of said allowed destination ports (see figure 1, elements 14-1..14-n 'output ports', of Arthurs).

Arthurs further discloses using the destination port bit map. However, Arthurs does not specifically mention generating the destination port bit map.

Arthurs discloses generating the physical port **availability** bit map. However, Arthurs does not specifically mention the physical port **security** bit map."

The Examiner relies for support on Arthurs' Fig. 3, and equates Arthurs' packet format (with a data field, source address field, destination bit-map field and priority bits field) to Applicant's "frame of digital data". Newton's Telecom Dictionary (24th Edition) (see page 398) defines "field" as "the specific location of data within a record". Newton's Telecom Dictionary (24th Edition) (see page 883) defines "string" as "a sequence of elements of the same type, such as characters, considered as a unit by a computer, a data structure composed of a sequence of characters".

As seen, Arthurs' Fig. 3 therefore discloses that each "field" (i.e., data <u>field</u>, source address <u>field</u>, destination bit-map <u>field</u> and priority bits <u>field</u>) is composed of a sequence of bits which correspond to the specific type of data as a "string".

The Applicant points out that the Examiner's above rejection arguments are deficient at least for the following reasons:

(A) The Examiner alleges that Arthurs' Fig. 3 (also see Arthurs col. 5, ll. 50-54) discloses Applicant's "destination port <u>bitmap</u>". The Applicant disagrees, and points out that the Examiner has failed to see that there is a difference between a "destination <u>bit-map field</u>" and a "destination port <u>bit-map</u>". The Examiner is referred to Newton's Telecom Dictionary (24th Edition) (see page 162), which defines a "Bitmap" as a "Representation of characters or graphics by **individual pixels arranged in row (horizontal) and column (vertical) order. Each pixel can be represented by one bit** ...." In other words, <u>Applicant's "destination port bitmap" is a "matrix" structure with bits arranged in rows and columns, where each bit represents a destination port location</u>.

As seen, Arthurs' Fig. 3 discloses a packet format (the alleged "frame of digital data") composed of a variety of "fields", namely, the data <u>field</u>, source address <u>field</u>, destination bit-map <u>field</u> and priority bits <u>field</u>, where each "field" is composed of <u>a sequence of bits</u> as a "string" of data. In other words, Arthurs' Fig. 3 at best, merely discloses a "string" of bits arranged as a "row" of bits within Applicant's "destination port bitmap" matrix structure. In this regard, the Examiner has misconstrued Applicant's

"destination port bitmap" as merely a "field" or a "row" of bits (such as Arthurs' "destination bit-map field").

(B) The Examiner relies for support on Arthurs' Fig. 6 (also see Arthurs col. 5, ll. 58-65, col. 6, ll. 4-9 and col. 7, ll. 1-3), and has incorrectly equated the "output availability field" and "source address field" during a sequential write to Arthur's token field format, to Applicant's "physical port security bit map" and "bitmap of allowed destination ports", respectively. As argued in Applicant's above section (A), that Applicant's "physical port security bit map" and "bitmap of allowed destination ports", are each separately a matrix structure which cannot be merely equated to a "field" or a "row" of bits.

(C) The Applicant initially points out that the entire reference of Arthurs is silent on "security", let alone disclosing the alleged "generating a physical port **security** bit map". Even though, the Examiner (see above Office Action), by his own admission concedes that "*Arthurs does not specifically mention the physical port **security** bit map*". Nevertheless, the Examiner's allegation that "*Arthurs discloses generating the physical port **availability** bit map*" is equally incorrect. The Examiner is simply referred to Applicant's above arguments (A) and (B) that Arthurs does not disclose any "bitmap" whatsoever.

In addition, the Examiner seems to have misconstrued Arthurs' Fig. 6 to an alleged "generating a physical port **availability** bit map of allowed destination ports". The Applicant points out that Arthurs' Fig. 6 discloses the **process of sequentially writing at**

the input ports (i.e., SA1 to SA8) **on Arthur's token field format structure** (i.e., source

address field (A_8, ..., A_1) and output availability field (a_8, ..., a_1)). More specifically, the

Examiner is referred to Arthur's Fig. 6 below:

FIG. 6

SA	d_8 ...d_1	A_8,	...	,A_1	a_8 ... a_1
1	01000100	0, 1, 0, 0, 0, 1, 0, 0			01000100
2	00001000	0, 1, 0, 0, 2, 1, 0, 0			01001100
3	10000001	3, 1, 0, 0, 2, 1, 0, 3			11001101
4	01010000	3, 1, 0, 0, 2, 1, 0, 3			11001101
5	00000011	3, 1, 0, 0, 2, 1, 0, 3			11001101
6	01000000	3, 1, 0, 0, 2, 1, 0, 3			11001101
7	00000000	3, 1, 0, 0, 2, 1, 0, 3			11001101
8	00100000	3, 1, 8, 0, 2, 1, 0, 3			11101101

The Examiner is also referred to the following citation of Arthurs (see col. 5, l. 58 to

col. 6, l. 20), which states the following:

> "The format of a typical token generated by the token generator 32 of
> FIG. 1 is illustrated in FIG. 3. **A token comprises two fields, a Source
> Address Field and an Output Availability Field**. The Output Availability
> Field comprises a bit a_i for each output port 144. A logic "1" in a
> particular bit position of the Output Availability Field indicates that the
> corresponding output port has been reserved. The token generator emits
> tokens with a cleared output availability field. The subfield A, in the
> Source Address Field of the token is the address of the input port whose
> packet will be transmitted to the ith output port (i.e. output port 14-i) if the

corresponding position a_a in the Output Availability Field is set equal to logic "1".

As indicated above, the control procedure comprises two phases in each transmission cycle: **a write phase at the input ports** and a read phase at the output ports. **At each input port, the write phase comprises a comparison of the Destination Bit Map Field of a packet with the Output Availability Field of the token**. The comparison results in the evaluation of $e_i + (d_i.a_i)$. The values taken on by e_i for different values of d_i and a_i are illustrated in FIG. 4. **The input port writes its source address into the ith subfield A, of the token Source Address Field** whenever $ei + 1$ for every i which $d_1 + 1$ in the packet header. **In other words, the subfield A, of the token Source Address Field is written with an input port address, if the packet header at that input port phase d_i +1 and if a_i is available and has not been previously reserved**. The input port also sets $a_i + 1$ to reserve the output port. **Each input port sequentially writes its information into the token during the first control phase**."

In brief, Arthur's Fig. 6 and the above citation disclose "*A token comprises two fields, a Source Address Field* (A_8, ..., A_1) *and an Output Availability Field* (a_8, ..., a_1)".

Also, Arthur's Fig. 6 discloses <u>a process of control procedure</u>, namely a write phase at the input ports which includes comparing two fields, namely, the "*Destination Bit Map <u>Field</u>* (d_8, ..., d_1)*of a packet with the Output Availability <u>Field</u>* (a_8, ..., a_1)*of the token*".

Arthurs further discloses that <u>the results of the fields comparison</u> (i.e., the information of each input port sequential writes) are written into the subfields (A_8, ..., A_1) of the Source Address Field (of the corresponding input port address SA(i)) if the packet header at that input port phase d_i +1 and if a_i is available and has not been previously reserved.

In this regard, Arthurs' Fig. 6 displays the sequential progress results of each subsequent "write" to the token at input port SA, where the Output Availability Field (a_8, ..., a_1) (the alleged "physical port security bit map") and the Source Address Field (e.g., (A_8, ..., A_1) (the alleged "bitmap of allowed destination ports") of the token may be updated and modified from port to port (if a_i is available and has not been previously reserved).

In other words, the Output Availability Field (a_8, ..., a_1) (the alleged "physical port security bit map") and the Source Address Field (e.g., (A_8, ..., A_1) (the alleged "bitmap of allowed destination ports") of the source input port SA1 is modified or updated, as soon as the token reaches the subsequent source input port SA2. Likewise, the Source Address Field (e.g., (A_8, ..., A_1) (the alleged "bitmap of allowed destination ports") of the source input port SA2 is modified or updated, as soon as the token reaches the subsequent source input port SA3 (a_i is available and has not been previously reserved).

In the scenario that a_i is not available and has been previously reserved (i.e., at input ports SA3 to SA7), the Output Availability Field (a_8, ..., a_1) (the alleged "physical port security bit map") and the Source Address Field (e.g., (A_8, ..., A_1) (the alleged "bitmap of allowed destination ports") are unchanged.

To summarize, Arthurs Fig. 6 (also see col. 5, l. 58 to col. 6, l. 20) discloses a token fields writing result (i.e., subject to updates and modification) on the Output Availability Field (a_8, ..., a_1) and Source Address Field (A_8, ..., A_1), as the writing phase progresses from one input port to the subsequent input port. Arthurs simply does not disclose the alleged "physical port security bit map" and the alleged "bitmap of allowed destination ports", contrary to the Examiner's allegation.

Based on the foregoing rationale of Applicant's arguments (A) to (C), the Applicant maintains that Arthurs does not disclose the alleged "destination port bitmap", "physical port security bit map" and "bitmap of allowed destination ports".

Moreover, the Applicant further submits that Arthurs' **process of sequentially writing at the input ports** (i.e., SA1 to SA8) **on Arthur's token field format structure** (i.e., source address field (A_8, ..., A_1) and output availability field (a_8, ..., a_1)), in fact, teaches away from Applicant's "bit map of allowed destination ports" and "physical port security bit map".

Accordingly, the Applicant also maintains that Arthurs also does not disclose or suggest the limitation of "generating a destination port bit map based on the destination address information contained in said frame of digital data; generating a physical port security bit map of allowed destination ports, wherein said physical port security bit map is generated based on one or both of information in said received frame of digital data and/or port security information associated with said network device; comparing, using

at least one logical operation, <u>said destination port bit map with said physical port</u> <u>security bit map to generate a bit map of allowed destination ports</u>," as recited by the Applicant in independent claim 1.

A(2) Sawey and Ross Are Not Combinable with Arthurs. Sawey and Ross Do Not Overcome Arthurs' Above Deficiencies

The Examiner (see Office Action, page 3) concedes that "*Arthurs does not specifically mention generating the destination port bit map*". The Examiner (see Office Action, page 3) looks to Sawey to overcome Arthurs' above deficiency, and states the following:

> "ii. Sawey teaches a crosspoint switch having multicast functionality, wherein Sawey discloses generating the destination port bit map **based on the destination address contained in the frame of the digital data** (see figure 4, elements 100 'receive multicast packet', 102 'generate port map mapping multicast address to destination output ports'; and column 7, lines 41-45, of Sawey)..."

(D) The Examiner relies for support on Sawey's flow chart in Fig. 4 (also see col. 7, ll. 41-45), and equates Sawey's "generating port map mapping multicast address to destination output ports" (*see* step (102)) to Applicant "<u>generating a destination port bit</u> <u>map</u> based on the destination address information contained in said frame of digital data," as recited in Applicant's claim 1. Sawey, nevertheless, is still deficient in not disclosing the alleged "physical port security <u>bit map</u>" and the alleged "<u>bitmap</u> of allowed destination ports".

The Examiner (see Office Action, page 3) further concedes that "*Arthurs does not specifically mention the physical port **security** bit map*". The Examiner (see Office

Action, pages 4-5) looks to Ross to overcome Arthurs' above deficiency, and states the

following:

> "On the other hand, Ross teaches a method for performing logical operations for packet processing, wherein **Ross discloses generating a physical port security bit map** based on information in said received frame of digital data (see column 3, line 58 to column 4, line 1 **'Thus, if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number [i.e., a physical port security bit map]**. Note that, as the rules are typically more complex than simple filters on port numbers, the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address [i.e., information of the packet], source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification.', of Ross, emphasis added).

> ...The ordinary skilled person would have been motivated to have applied the teaching of Ross into the system of Arthurs to generate the physical port security bit map, because **Arthurs teaches** "Illustratively, the electronic control network is in the form of a track which **sequentially links all of the input ports and output ports. At the beginning of the track is a token generator which generates control tokens. The control tokens are passed sequentially around the track from port to port.**" (see column 2, lines 58-63, of Arthurs, emphasis added). Ross teaches "The present invention generally concerns data communications systems, in particular internetworking systems and specifically access control techniques for such systems." (see column 1, lines 13-15, of Ross, emphasis added). Therefore, Ross's teaching could enhance Arthurs's system, because **"the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address [i.e., information of the packet], source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification."**

(E) It is unclear which element of Ross is specifically equated by the Examiner to

Applicant's "physical port security bitmap". The Examiner seems to argue that Ross

discloses using a rule to check for each entry within a CAM (content addressable memory), and the rule may "deny packets" based on a port number 80 within one of the CAM entries. In other words, the Examiner seems to equate Ross' CAM entries (which include multiple fields) to an alleged "physical port bitmap", and Ross' CAM entries being checked by the rules, to Applicant's "physical port <u>security</u> bitmap".

The Applicant disagrees, and refers the Examiner to the citation of Ross (see col. 3, l. 53 to col. 4, l. 1), which states the following:

> "In the context of ACL filtering, CAMs are used to hold bit masks representing elements of the ACL rules. The various rule elements are each implemented by one or more entries in a CAM. For example, <u>the rule element "eq" is the simplest CAM entry, because a CAM is designed to test for equivalence between the key and each entry in the CAM</u>. Thus, **if the rule is "deny packets from port 80," the corresponding CAM entry is a bit string representing a value of 80 in the portion of the string corresponding to the port number**. Note that, as the rules are typically more complex than simple filters on port numbers, <u>the CAM entries typically consists of multiple fields corresponding to the parts of the conventional flow label of a packet. Such fields typically include the IP source address, IP destination address, source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification</u>.

Even though Ross discloses using a rule to "deny packets" (the alleged 'security") based on a port number of value 80 in one of the entries in a CAM (content addressable memory), Ross' CAM entries, nevertheless, cannot be equated to an alleged "physical port bitmap".

More specifically, Ross (see Ross' table 1 and 2) discloses that "*the CAM entries typically consists of <u>multiple fields</u> corresponding to the parts of the conventional flow*

label of a packet". Examples of such multiple fields include "*the IP source address, IP destination address, source port number, destination port number, type of service (TOS), and Layer 3 and Layer 4 protocol identification*". In other words, Ross' CAM entries form a table composed of various fields of a <u>flow label</u> of TCP/UDP packet, which is not the alleged "physical port bitmap" (since a bitmap is a matrix structure with rows and columns of bits representing physical ports).

Based on the foregoing rationale that Ross' CAM entries are merely a <u>flow label</u> of TCP/UDP packet, the Applicant maintains that Ross' CAM entries cannot be equated to the alleged "physical port <u>security</u> bit map".

(F) Furthermore, Applicant's claim 1 clearly recites a "physical port <u>security</u> bit map of <u>allowed destination ports</u>". Ross' alleged "security" rule, instead discloses an exact opposite function, namely, "denying" a packet from transmitting based on a certain physical port number within a packet entry. In this regard, the Applicant also maintains that Ross' CAM entries with the rules cannot be equated to the alleged "physical port <u>security</u> bit map of <u>allowed destination ports</u>", and Ross fails to overcome Arthurs' deficiency in failing to disclose the alleged "physical port security <u>bit map</u>" and the alleged "<u>bitmap</u> of allowed destination ports".

A(3) The Combination of Arthurs, Sawey and Ross still Does Not Disclose All the Elements of Applicant's Claim 1.

Based on at least the above arguments (A) to (F), the Applicant maintains that the combination of Arthurs, Sawey and Ross still does not disclose or suggest at least the limitation of "generating a physical port security bit map of allowed destination ports, wherein said physical port security bit map is generated based on one or both of information in said received frame of digital data and/or port security information associated with said network device; comparing, using at least one logical operation, said destination port bit map with said physical port security bit map to generate a bit map of allowed destination ports," as recited by the Applicant in independent claim 1.

Accordingly, the proposed combination of Arthurs, Sawey and Ross does not render independent claim 1 unpatentable, and a *prima facie* case of obviousness has not been established. The Applicant submits that claim 1 is allowable.

Independent claim 12 is similar in many respects to the method disclosed in independent claim 1. Therefore, the Applicant submits that independent claim 12 is also allowable over the references cited in the Office Action at least for the reasons stated above with regard to claim 1.

B. Rejection of Dependent Claims 2-11 and 13-24

Based on at least the foregoing, the Applicant believes the rejection of independent claims 1 and 12 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Arthurs in view of Sawey and further in view of Ross has been overcome

and requests that the rejection be withdrawn. Additionally, claims 2-11 and 13-24 depend from independent claims 1 and 12, respectively, and are, consequently, also respectfully submitted to be allowable based on the above arguments.

II.   Response To Examiner's Arguments

The Applicant believes that the above arguments (A) to (F) in section I have fully addressed the Examiner's arguments in the Examiner's Response. In addition, the Applicant maintains any applicable remaining arguments in part of in full in the previous response dated 1/10/2011.

In general, the Office Action makes various statements regarding claims 1-24 and the cited references, which statements are now moot in light of the above. Thus, the Applicant will not address such statements at the present time. However, the Applicant expressly reserves the right to challenge such statements in the future should the need arise (e.g., if such statement should become relevant by appearing in a rejection of any current or future claim).

CONCLUSION

Based on at least the foregoing, the Applicant believes that all claims 1-24 are in condition for allowance. If the Examiner disagrees, the Applicant respectfully requests a telephone interview, and requests that the Examiner telephone the undersigned Patent Agent at (312) 775-8093.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

A Notice of Allowability is courteously solicited.

Respectfully submitted,

Date: June 16, 2011
           / Frankie W. Wong /

           Frankie W. Wong
           Registration No. 61,832
           Patent Agent for Applicant

MCANDREWS, HELD & MALLOY, LTD.
500 WEST MADISON STREET, 34TH FLOOR
CHICAGO, ILLINOIS 60661
(312) 775-8093 (FWW)